DRAFT

Interoperability: Is It Achievable?

Anthony W. Faughn
April 2001

Program on Information Resources Policy

Center for Information Policy Research

Harvard University

The Program on Information Resources Policy is jointly sponsored by Harvard University and the Center for Information Policy Research.

April 2001

PROGRAM ON INFORMATION RESOURCES POLICY

Harvard University **Center for Information Policy Research**

Affiliates

Anonymous Startup
AT&T Corp.
Australian Telecommunications Users Group
BellSouth Corp.
The Boeing Company
Booz-Allen & Hamilton, Inc.
Carvajal S.A. (Colombia)
Center for Excellence in Education
CIRCIT at RMIT (Australia)
Commission of the European Communities
Critical Path
CyberMedia Convergence Consulting
CyraCom International
DACOM (Korea)
ETRI (Korea)
eYak, Inc.
Fujitsu Research Institute (Japan)
GNB Technologies
Grupo Clarin (Argentina)
Hanaro Telecom Corp. (Korea)
Hearst Newspapers
High Acre Systems, Inc.
Hitachi Research Institute (Japan)
IBM Corp.
Intel Corp.
Korea Telecom
Lee Enterprises, Inc.
Lexis-Nexis
Eli Lilly and Co.
Lucent Technologies
John and Mary R. Markle Foundation
McCann North America
Microsoft Corp.
MITRE Corp.
Motorola, Inc.
National Security Research, Inc.
National Telephone Cooperative Assoc.
NEC Corp. (Japan)
NEST–Boston
Nippon Telegraph & Telephone Corp (Japan)
NMC/Northwestern University
Research Institute of Telecommunications and Economics (Japan)
Samara Associates
Siemens Corp.
SK Telecom Co. Ltd. (Korea)
Strategy Assistance Services
TRW, Inc.
United States Government:
 Department of Commerce
  National Telecommunications and Information Administration
 Department of Defense
  Defense Intelligence Agency
  National Defense University
 Department of Health and Human Services
  National Library of Medicine
 Department of the Treasury
  Office of the Comptroller of the Currency
 Federal Communications Commission
 National Security Agency
 United States Postal Service
Upoc
Verizon

Disclaimer

The views, opinions, and conclusions expressed in this paper are those of the author and should not be construed as an official position of the United States Air Force, the Department of Defense, or any other government agency or department.

Contents

Chapter One: Interoperability

> *In the 1960s, the Sixth Fleet Commander, Admiral Kidd in the Mediterranean, used to die for information. The system was clogged up. He couldn't get information. Then every day he used to see this plane flying over the Mediterranean. It was an Air Force reconnaissance plane. It used to dip its wings to him. That plane had all the information he needed. They couldn't talk. Simple solution and a couple young officers got medals. They put a compatible communications system on the plane and the ship. They solved it. The people thought they were heroes. Twenty years later, the same problem. A different part of the world; Air Force planes flying over a Navy ship; they couldn't talk to each other. You fix it by doing the same thing that was done 20 years ago. We sometimes just don't learn our lessons about communications problems.*[1]

Admiral Kidd was referring to the interoperability problems associated with Operation Urgent Fury or the Grenada Invasion, in which the press highlighted the interoperability shortfalls among U.S forces that became the catalyst for legislation and changes in policy, guidance and procedures and numerous attempts to solve issues along the long road of trying to achieve Joint interoperability.

1.1 Introduction

> *Despite long-standing existence of DOD policy on interoperability and a process for interoperability certification, interoperability problems persist. A report on the 1999 Operation Allied Force (Kosovo) cited numerous combined-interoperability problems.6 A General Accounting Office (GAO) report identified weaknesses in the DOD's interoperability certification process. The Commanders-in-Chief (CINCs) of the Unified Commands have frequently raised interoperability issues via the Joint Staff's Joint Warfighting Capability Assessment (JWCA) process, the CINC Interoperability Program Offices (CIPOs), and other fora.*[2]

---

[1] Fred R. Demech, Jr., Career Cryptologist; former Commanding Officer, US Naval Security Group Activity, Edzell, Scotland, (1987, pp. 125-146), "Making Intelligence Better," in Thomas P. Coakley, ed., *C3I: Issues of Command and Control*, National Defense University Press, Washington D.C., 1991, 163

[6] Kosovo/Operation Allied Force, report in draft as of December 1999.

[2] Jacques S. Gansler, USD AT&L, Arthur L. Money, ASD C3I, Philip E. Coyle, Director, OT&E, VADM S. A. Fry, Director, Joint Staff, memorandum for Secretaries of the Military Departments, USD for Policy, USD (Comptroller/Chief Financial Officer), ASD for Legislative Affairs, General Council, subject: Promulgation of DOD Policy For Assessment, Test, and Evaluation of Information Technology System Interoperability, December 4, 2000.

How is it possible that after all the effort and money spent in the 15 years since the fiasco in Grenada there are still problems with interoperability in Kosovo? How did the problem evolve? Why are CINCs and service staffs still concerned with interoperability?

Interoperability was not as much a problem during World War II because the United States had essentially no military equipment when it entered the war. The government had to purchase practically everything at the same time, and naturally, bought the same equipment for all the services–whether that equipment was ultimately fielded in ships, tanks, or airplanes. By default, therefore, the services achieved interoperability.[3]

In the 50+ years since World War II, budget constraints resulted in the United States services not being able to replace all their systems completely at the same time, even if they had wanted to. Instead, each service had to procure individual systems that optimally supported its own activities at separate times. This approach resulted in different generations of equipment that did not interoperate with the materiel and systems of the other services. It caused no or minimal difficulties, and probably even improved performance, when the services operated more or less autonomously. However, with the advent of joint operations the interoperability problem became readily apparent.

Lessons learned from and debates over the successes of joint U.S. operations encompassing the past two decades between 1980 and 2000—Grenada; Persian Gulf War; African operations in Somalia, Rwanda, and Liberia; Bosnia; and Kosovo— all highlight problems with interoperability among the U.S. forces and between U.S. forces and allied or coalition forces.

Today major interoperability problems still exist in theaters with the greatest potential for conflict despite the tremendous planning and expenditure of funds to ensure it. The latest Joint Vision document, Commanders-in-Chief (CINCs) of the unified and specified commands, service chiefs, congressmen, etc., espouse the importance of and mandate interoperability. The efforts of numerous DOD efforts such as the Quadrennial Review (QDR) are focused on achieving interoperability. In attempts to mitigate the impacts of factors that hamper achieving interoperability, new policy and guidance has been promulgated, organizational roles such as Joint Forces Command redefined and evolutionary acquisition processes implemented. Although the jury will be out for several years to determine if the newest efforts will help to achieve interoperability they are still relevant to the discussion as they will guide the attempts to attain interoperability.

1.2 Scope and Organization

Despite the efforts exerted in trying to achieve interoperability it is near impossible to find a single concise document dedicated to the problem of interoperability. Research found only two

[3] Dr. David W. Phillips, Ph.D., Joint C4ISR Decision Support Center, interview with author, January 19, 2001.

studies associated with interoperability conducted in the past 25 years. The first study, accomplished for the Department of Defense (DOD) by the Institute for Defense Analyses (IDA) and published in 1976, now declassified and amazingly relevant, is still not releasable outside IDA. The other, more recent paper--directed by Congress in 1996; conducted by the Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council (NRC); and published in 1999 by the Committee to Review C4I Plans and Programs[4] is lengthy and technically oriented.

With this in mind, the purpose of this effort is to present a shorter and more available product that captures at the macro-level the major issues associated with achieving interoperability.

Following this introductory chapter, the second chapter will define interoperability and address its relationship to other, often-confusing terms: compatibility and integration. Chapter three will set the stage by discussing the importance of interoperability as seen through a review of lessons learned from past operations, its continued importance to joint operations and senior leadership, and its impact on future operations. The fourth chapter will present factors that contribute to or hamper the achievement of interoperability. This chapter is the heart of the paper. It will discuss the impacts of rapidly changing technology, the changing nature of operations, competing priorities, inadequate oversight, and poor joint training and exercises. Chapter five will present mitigating initiatives aimed at improving interoperability among the services. These include changes in policy and guidance, organizational roles, and acquisition process. The sixth and last chapter will provide a brief summary and draw conclusions as to whether, based on the past, we can expect the latest attempts to improve or solve the interoperability dilemma to succeed or fail.

[4] National Research Council [NRC], Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, Committee to Review DOD C4I Plans and Programs, *Realizing the Potential of C4I: Fundamental Challenges,* National Academy Press, Washington D.C., December 1999; also available on-line at URL: http://bob.nap.edu/html/C4I/html.

Chapter Two: Definitions

2.1 Definitions of Interoperability

2.1.1 Operational and Technical Definitions

The Joint Publication 1-02, which is the Department of Defense Dictionary for Military Terms and that serves as the core document for the services and agencies to refer to if there is a question of definition, defines both operational and technical interoperability. It defines *operational interoperability* as, "the ability of systems, units, or forces to provide services to and accept services from other systems, units, or forces and to use the services so exchanged to enable them to operate effectively together."[1] *Technical interoperability* is defined as, "the condition achieved among communications-electronics equipment when information services can be exchanged directly and satisfactorily between them and /or their users."[2]

The 1999 report of the congressionally mandated study of C4I, *Realizing the Potential of C4I: Fundamental Challenges*, further explains the differences in operational and technical interoperability. In reference to operational interoperability it states, "operational interoperability addresses support to military operations and, as such, goes beyond systems to include people and procedures, interacting on an end-to-end basis."[3] As for technical interoperability it states that, "interoperability at the technical level is essential to achieving operational interoperability" and is "an issue that arises between two systems rather than organizations."[4]

Technical interoperability stops at the systems. If the two or more systems can exchange data then they are considered technically interoperable. However, operational interoperability adds the user and says that the information exchange is between two or more users who must be able to do more than just exchange information, but also be able to understand the information. Understand is the key word. For example, if one commander is German and one is U.S. and they exchange just information then it does no good unless the German officer can read and speak English or vice versa. The information must be converted at each end so that it is understandable to achieve operational interoperability.

---

[1] Joint Publication 1-02, *Department of Defense Dictionary of Military Terms*, [as amended], US Government Printing Office, Washington DC, December 7, 1998; also available on-line at URL: http://www.dtic.mil/doctrine/jel/doddict

[2] Ibid.

[3] National Research Council [NRC], Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, Committee to Review DOD C4I Plans and Programs, *Realizing the Potential of C4I: Fundamental Challenges,* National Academy Press, Washington D.C., December 1999; also available on-line at URL: http://bob.nap.edu/html/C4I/html, Chapter 2, 1.

[4] Ibid,, Chapter 2,2.

2.1.2 Relationship with Compatibility and Integration

Often when discussing interoperability the terms "compatibility" and "integration" can confuse the interoperability definition. Rear Admiral R. M. Nutwell, in his presentation on "Achieving Joint Information Interoperability," explains these related concepts well. He states:

> *Integration* is generally considered to go beyond mere Interoperability to involve some degree of functional dependence. For example, a mission planning system might rely on an external intelligence database; an air defense missile system will normally rely on acquisition radar. While interoperable systems can function independently, an integrated system loses significant functionality if the flow of services is interrupted. An integrated family of systems must of necessity be interoperable, but interoperable systems need not be integrated.
>
> *Compatibility* is something less than Interoperability. It means that systems/units do not interfere with each other's functioning. But it does not imply the ability to exchange services. Interoperable systems are by necessity compatible, but the converse is not necessarily true. To realize the power of networking through robust information exchange, we must go beyond compatibility.[5]

Admiral Nutwell further explains,

> "In sum, Interoperability lies in the middle of an 'Integration Continuum' between compatibility and full integration. It is important to distinguish between these the fundamentally different concepts of compatibility, interoperability, and integration, since failure to do so sometimes confuses the debate over how to achieve them. While compatibility is clearly a minimum requirement, the degree of interoperability/integration desired in a Joint family of systems or units is driven by the underlying Operational Concept, as well as by Family of Systems (FoS) design and cost/effectiveness tradeoffs."[6]

[5] RADM R. M. Nutwell, US Navy, Deputy Secretary of Defense for Command, Control, Communications, and Intelligence Surveillance, and Reconnaissance Systems, "Achieving Joint Information Interoperability," Version 1, April 4, 2000, 3.

[6] Ibid.

Chapter Three: Importance of Interoperability

3.1 Operations over the Past Two Decades and the Future

A look at the past two decades of U.S. joint operations highlights the importance of interoperability. Although Grenada drew attention to the problem, interoperability was important and a goal even before the Grenada Invasion. In a 1982 address to Harvard University's John F. Kennedy School of Government Seminar on Command, Control, Communications, and Intelligence (C3I), Hillman Dickinson, the former Director of Command, Control, and Communications Systems for the Joint Chiefs of Staff, listed "improve joint and combined interoperability" as the second of eight priorities "because the services have to work together if we have to fight; you can't fight separately."[1] Little did he know that the validity of this statement would be demonstrated in a realistic environment less than a year later in Grenada.

3.1.1 Grenada

The Grenada operation in 1983 provided a practical test of the extent to which interoperability was achievable by joint forces operating together on short notice and for the first time. Significant problems of interoperability during the operation were reported in the press. No unclassified official reports detail the problems that actually occurred or describe the specific actions taken to prevent the same problems from occurring in the future. However, unclassified lessons learned highlighted the problem:

> The final challenge to invading forces was the lack of a fully integrated, interoperable communications system. Communications was to have been the glue that would tie together the operation of four independent United States military service elements; however, communications support failed in meeting certain aspects of the mission.[2]

Although there were shortages in communications, interoperability was a major problem during the invasion. For example:

> … the uncoordinated use of radio frequencies caused a lack of interservice communications except through offshore relay stations and prevented radio communications between Marines in the north and Army Rangers in the south. As a result, Marine commanders were kept unaware for a long

---

[1] Hillman Dickinson, Planning for Defense-Wide Command and Control, in Seminar on Command, Control, Communications and Intelligence, Guest Presentations—Spring 1982, Harvard University Program on Information Resources Policy, Cambridge, Mass., I-82-3, December 1982, 23; also available on-line at URL: http://www.pirp.harvard.edu/publications.html.

[2] Frank M. Snyder, *Command and Control The Literature and Commentaries*, National Defense University Press, Fort Lesley J. McNair, Washington D. C., September 1993, 111.

> time that Rangers were pinned down without armor support. In a second incident, it was reported that one member of the invasion force placed a long distance phone call to Fort Bragg, N.C., to obtain C-130 gunship support for his unit which was under fire.[3] Commenting overall on the issue of interoperability, Admiral Metcalf, the Commander-in-Chief of Atlantic Command and the overall commander for the operation, wrote, 'In Grenada we did not have interoperability with the Army and the Air Force, even though we had been assured at the outset that we did.' … An instruction on interoperability was subsequently issued by the Secretary of Defense, as well as a memorandum of policy on the same subject by the Joint Chiefs of Staff, and the general 'backwash' from the operation may have contributed to the congressional concerns that led to the DOD Reorganization Act of 1986.[4]

Grenada became the catalyst for programs aimed at fixing the problem. Donald Latham, the former Assistant Secretary of Defense for Command, Control, Communications, and Intelligence, speaking to the same seminar in 1985, commented that:

> …if you want to talk across services (and that came up in Grenada, about cross service communications with different types of radios, using different types of COMSEC equipment) you're probably going to be in trouble. … However, we do have a new program called Joint Interoperability of Tactical Command and Control Systems (JINTACCS) which is a joint, cross service effort to make sure that tactical command and control systems are, in fact, interoperable. We will spend about $100 million on that in 1986 doing tests, promoting standards, setting up various testbeds, doing simulations, and trying to be the keepers of the interoperability."[5]

Within five years this program would be tested in the aftermath of Saddam Hussein's invasion of Kuwait.

---

[3] Colonel Stephen Anno and Lieutenant Colonel Willaim E. Einspahr, *Command and Control Lessons Learned: Iranian Rescue, Falklands Conflict, Grenada Invasion, Libya Raid*, Chapter IV, "The Grenada Invasion", Air War College Research Report, No. AU-AWC-88-043, Air University, Maxwell Air Force Base, Alabama, [reprinted as an extract from by The United States Naval War College Operations Department, NWC 2082, http://www.fas.org/man/dod-101/ops/urgent_fury.htm], accessed last on February 5, 2001, 36.

[4] Frank M. Snyder, 111.

[5] Donald Latham, A View from inside OSD, in Seminar on Command, Control, Communications and Intelligence, Guest Presentations—Spring 1985, Harvard University Program on Information Resources Policy, Cambridge, Mass., I-86-1, February 1986, 121; also available on-line at URL: http://www.pirp.harvard.edu/pubs.html.

3.1.2 Persian Gulf War

Desert Shield and Desert Storm provided real world tests of U.S. forces' ability to operate jointly as codified in the Goldwater-Nichols Act of 1986 and as tests for equipment designed to ensure interoperability among the services. These tests were not without interoperability problems among the U.S. forces.

> The interim report by the Secretary of Defense on the C3 systems of U.S. and coalition forces during the Persian Gulf Conflict deserves to be read carefully…. [A]lthough superseded by a "final report" for the Secretary of Defense 1 April 1992 … the interim report is retained as a reading because it is fresher, more informative, and covers the issues more frankly…. The general tone is one of accomplishment, even claiming for the C3I system much of the success of Desert Storm. Yet despite the upbeat language, it is clear that greater attention will need to be paid to plans for … a greater measure of interoperability.[6]

Les Aspin and William Dickinson, in their *Defense for a New Era, Lessons Learned of the Persian Gulf War*, highlighted the depth of the problem:

> Operation Desert Storm demonstrated that tactical communications are still plagued by incompatibilities and technical limitations. At CENTCOM corps and wing levels, a significant portion of the war was conducted over commercial telephone lines because of the volume and compatibility limitations of the military communications system…. Communications were worse in the field….[7]

The tri-service tactical (TRI-TAC) communications equipment, acquired by a program started in the late 1970s and fielded in the 1980s in an effort to ensure interoperability, had its share of problems. The Army's unclassified lessons learned highlighted a major problem with the difference in the planning tools used by the Air Force and the joint community and those used by the Army in setting up the TRI-TAC communications architecture hubs—the circuit and message switches which provided the command and control backbone. The Army used the objective TRI-TAC network planning and management tool, which had undergone and successfully passed a User's Acceptance Test in July 1990. However, because of constraints on physical size, the Air Force and joint community chose not to adopt the objective tool and instead adopted another as their interim solution. As a result, few or no products for network planning and management could be exchanged electronically between the various organizations, resulting in lack of timely information exchange, inconsistent circuit routing lists, inconsistent circuit and message switch

[6] Frank M. Snyder, 79.

[7] Ibid, 71.

data bases, lack of a Theater Tactical Telephone Directory, and lack of accurate theater-level network diagrams.[8]

The Army's lessons learned also highlighted additional interoperability problems associated with the joint force concept:

> There was no data conversion and translation between the information received via JTIDS (Joint Tactical Intelligence Data System) in the Airborne Warning and Control System (AWACS) for transmission on the TADIL-A (downlink circuit) net. Conversely, information received via TADIL-A in the AWACS was not available for conversion to the JTIDS net.[9]

The Navy had its problems also. Most notable was its inability to receive the Air Tasking Order (ATO) electronically, which meant that the ATO had to be printed as hard copy and then delivered to the fleet via helicopter. According to the unclassified Navy's lessons learned, "… problems were encountered, particularly in command and control, communications, interoperability." The Joint Forces Air Component Commander (JFACC) in charge of prosecuting the air war and in charge of all services' airplanes and air taskings, used the ATO as a centralized planning and execution tool, which was effective in managing a high volume of sorties generated to concentrate coalition airpower against Iraq. However, "…there were some problems with production of the ATO and its delivery to naval forces."[10]

3.1.3 African Operations in the 1990s

Lessons learned from the 1990s African operations illuminate the difficulty with interoperability among multinational forces, especially with developing countries, and with international organizations associated with the changing nature of military operations and operations other than war. Lessons learned from the 1991 Somalia "Restore Hope" operation emphasized the challenges associated with working with other countries and organizations:

> The most significant potential of interoperability problems occurred between U.S. forces and the multinational contingents…Equipment considered standard—even basic—in most western armies is simply not present in the inventories of many military contingents from developing countries … The equipment multinationals do bring with them is not likely to be interoperable … [C]rossing over the 'seams' of national control

[8] Interoperability, Joint Tactical Communications (TRI-TAC), http://call.army.mil/call/newltrs/92-1/92-1ch3.htm, accessed November 2, 2000, Chapter 3, np.

[9] Ibid.

[10] U.S. Navy in Desert Shield/Desert Storm, VI Lessons Learned and Summary, Department of the Navy, Naval Historical Center, Washington D.C., 1.

> created severe interoperability problems—a situation that occurred whenever one national contingent had to cross over the boundary to reinforce another. [11]

Somalia also revealed interoperability problems between U.S. forces. The lessons learned highlighted that, while "The internal problems affecting U.S. forces did not involve any Grenada-like operational fiascoes; however, the ones that did occur underline the continuing problem of aligning equipment, procedures, and standards in the joint environment."[12] The UNITAF, a Marine-generated headquarters, used obscure word-processing software, while CENTCOM, like most other military users, preferred a different and most modern one. At the headquarters level, a similar difficulty plagued exchanges of email. At the tactical level, the ATO formats differed between the east and west coast ships of the Marine Amphibious Ready Group. Most serious was that the same Army and Marine single-channel tactical radios acquired compatibility problems caused by differing upgrades, which resulted in the Army hospital in Mogadishu not being able to talk to the Navy offshore for the first 3 weeks of the operation.[13]

Three years later, the 1994 Rwanda lessons learned again captured the interoperability challenges of dealing with multinational forces as well as various private volunteer organizations and non-governmental organizations.

> Although organizations were adept at intraorganizational communications procedures, interorganizational communications dragged because of dissimilar communications equipment, platforms, frequencies, and protocols. The lack of interoperable hardware and peripherals, common standards, and protocols was the main obstacle to looped communications and to reliable and broad-based security in the field.[14]

Liberia echoed similar problems and highlighted the cost involved in achieving interoperability with emerging nations. Lessons learned emphasized that, "Lack of funding for communications will further exacerbate this situation… Although lateral communications in the field seems imperative, the lack of interoperability continues to impede communications, whether by radios or computers."[15]

---

[11] Kenneth Allard, *Somalia Operations: Lessons Learned*, II. Operational Lessons Learned, National Defense University Press, Washington D.C., 1995; also available on-line at URL: http://www.ndu.edu/inss/books/allardch2.html, accessed January 2, 2001, 1,6.

[12] Ibid, 23.

[13] Ibid, 24.

[14] Managing Communications: Lessons from Interventions in Africa, http://www.usip.org/oc/sr/managingcomm4.html , accessed January 2, 2001, 29.

[15] Ibid, 31.

3.1.4 Operation Desert Fox

Seven years after Desert Shield/Storm and after the African series of operations other than war, the United States found itself once more engaged in combat actions against Saddam Hussein and Iraq in Operation Desert Fox. Again, interoperability became a major issue in the planning and execution, highlighting that interoperability still eluded achievement. Desert Fox also showed that despite improvements and dependence on technology a small snafu could have a major impact. This time the source of the interoperability problem concerned a glitch with the common operational picture, intended to give the operational commander a complete picture of the battlespace and forces, which had been a major focus of programs over the seven-year interim period. A CNN article captured the significance and potential impact of a "small" glitch:

> Because of a glitch…GTN [Global Transportation Network] presented military planners at three commands with two different operational pictures…Although GTN was designed to automatically process updates within 30 seconds, a software problem such as the one experienced in Desert Fox could cause a significant drop in responsiveness and hinder the ability to make 'on the spot' decisions…The problem occurred when a data field from the Joint Operations and Planning System (JOPES)—a Multiservice system that provides the military with a standard format and language for planning military operations—failed to convert properly when it reached GTN. This failure presented planners with false information on the status of cargo aircraft…Although GTN never went down, the interoperability problem caused some confusion when the Air Mobility Command (AMC) and U.S. Central Command were working with different information than TRANSCOM was using…If GTN were to fail, users would be forced to resort to the use of fax machines, phones and other manual methods, and users would have to make do with old information. [16]

Martin Libicki, a defense analyst with Rand Corp. specializing in information warfare and information operations, said he was surprised that a small glitch such as the one with the JOPES-GTN interface could happen, given the state of the art technology. "We've been doing this [database technology] for years," he said.[17]

3.1.5 Kosovo

Kosovo serves as the latest example of shortfalls in interoperability under combat conditions. In particular, it highlighted the increasing interoperability gap between the U.S. and allied or multinational forces. While there were still documented problems associated with U.S.

---

[16]Daniel Verton, "Software snafu slowed key data during Iraqi raid," February 25, 1999, http://cnn.com/TECH/computing/9902/25/iraqi.idg/index.html, accessed on November 9, 2000.

[17] Ibid.

interservice interoperability the lessons learned highlight the growing difference in technology between the U.S. and its allies.

In a joint statement to the Senate Armed Services Hearing on Kosovo, the senior leadership for both the U.S. and NATO forces identified interoperability as an impediment among allied forces. General Wesley Clark, NATO Supreme Commander; Admiral James Ellis, Commander of Allied Forces—Southern Europe, and Lieutenant General Michael Short, Commander of Allied Forces—Central Europe, had this to say:

> Finally, Operation Allied Force illuminated the capability gaps between the U.S. military and our NATO allies. For example, not all NATO nations possess adequate … secure communications… These gaps impeded interoperability among Allied forces during the campaign…Ultimately, NATO nations need to upgrade their militaries to ensure they remain compatible with U.S. Forces.[18]

3.1.6 Future Operations and Wars

As the lessons learned from Kosovo indicate, the absence of interoperability will impede future NATO and European operations. However, the Pacific theater has equal if not greater future problems.

A January 8, 2001, *Defense News* article, although Army centric, highlighted the problem in Korea and the Pacific theater, where the United States expects its forces may have to fight and where we plan for one of the two major theater wars. The article drives home the relevance of interoperability in a part of the world where DOD currently focuses much of its planning and where the potential exists to be at war very quickly, giving the deploying forces little time for preparation and requiring them to come as they are. It highlights that:

> Old, incompatible command and control systems are preventing U.S. Army from sharing information in a timely manner with other regional services and allies...These disparate systems, known as stovepipe systems, perform only one function and do not share information with other voice, video, and computer systems. This means Army leaders in the region must make decisions using data that sometimes is two to four hours old in an era when battlefield and intelligence information changes by the second, industry and military officials say.[19]

---

[18] "Joint Statement to Senate Armed Services Hearing on Kosovo: Lessons Learned," *The U.S. Mission to NATO Security Issues Digest*, No. 203, October 21, 1999, 6.

[19] Frank Tiboni, "Slow Systems Hinder U.S. Pacific Forces, Allies, *Defense News*, Times News Group Incorporated, Springfield, Virginia, January 8, 2001, 12.

The article quoted Lieutenant General Ed Smith, Commanding General of U.S. Army Forces Pacific, as saying:

> U.S. Army Pacific Command (USARPAC), Honolulu, also receives untimely information from U.S. services and ally countries in the region because of its stovepipe C4 systems … 'We need to minimize the interoperability gaps,' Smith said, 'We need to think joint, not Army…The Army should not think in terms of integrating its C4I systems service-wide, but rather linking its future systems with those of other services and countries, he said.[20]

The problem is not isolated to the Korean peninsula. According to retired Brigadier General Jack Schmitt, currently vice president of Army systems integration at Burdeshaw Associates, "Inadequate C4I connections complicate Army interoperability with other countries in the Asia and Pacific theaters."[21]

3.2 Continuing Importance of Interoperability

The United States no longer plans to fight in such a way that individual services would each conduct their own operations, as they did in Korea or Vietnam. Instead the United States plans on joint operations. In the aftermath of the invasion of Grenada, which was codified by the Goldwater-Nichols Act of 1986. As noted earlier, a major catalyst for the legislation was the lack of interoperability. The act, in its sweeping reorganization for the Department of Defense, established by law that all future operations would be joint. This meant that these forces will require joint command and control and therefore that interoperability will be "…a key enabler for the conduct of effective, collaborative, multi-service military operations..."[22]

---

[20] Frank Tiboni, "Slow Systems Hinder U.S. Pacific Forces, Allies, *Defense News*, Times News Group Incorporated, Springfield, Virginia, January 8, 2001, 12.

[21] Ibid.

[22] Realizing the Potential of C4I, Chapter 2, 1,4.

3.2.1 Joint Operations

> *True joint C2 requires not only that the force components from various services be able to communicate with the Joint Task Force headquarters, but that they also have effective tactical communications among each other ... Access to the Air Tasking Order should not require resorting to paper, as in DESERT STORM and Kosovo ... The first step toward a genuinely joint C2 system that fully leverages the potential of IT is interoperability.*[23]
>
> Victor A. DeMarines
> President, The MITRE Corporation (Retired)

As a result of the shift to joint operations, the visions, policy, doctrine, tactics, and procedures have evolved to embrace interoperability. Both *Joint Vision 2010* and *Joint Vision 2020* espouse the necessity for interoperability. *Joint Vision 2020*, released in June 2000, reiterates the importance of interoperability for successful multinational and interagency operations. In dedicating a complete section of the short (36-page) document to interoperability, it underscores the need to improve interoperability and establishes the mandate for doing so:

> Interoperability is the foundation of effective joint, multinational, and interagency operations. The joint force has made significant progress toward achieving an optimum level of interoperability, but there must be concerted effort toward continued improvement…. Interoperability is a mandate for the joint force 2020—especially in terms of communications … and information sharing…. [a]s with multinational partners, interoperability in all areas of interaction is essential to interagency operations.[24]

3.2.2 Senior-level Focus

A key indicator of importance is where senior-level staffs (e.g., the Office of the Secretary of Defense (OSD), the Joint Staff, etc.) focus their attention. Within the last 18 months, top-level staffs have dedicated significant effort to drafting, coordinating, and publishing updated policy concerning interoperability. For example, the January 4, 2001, DOD 5000 series instructions that provide acquisition policies and guidance and the recently updated Chairman of the Joint Chiefs of Staff Instructions (CJCSIs) for the requirements process all mandate a more stringent requirements and acquisition process to ensure interoperability. (For a further discussion of these documents, see **Chapter Five**.)

---

[23] Victor A. DeMarines, "Exploiting the Internet Revolution," in Carter, Ashton B. and White John P., eds., *Keeping the Edge Managing Defense for the Future*, MIT Press, Cambridge, Mass., September 2000, 66.

[24] Vision Statement, "Joint Vision 2020", US Government Printing Office, Washington DC, June 2000, 21.

A look at the recent effort behind the production *Joint Vision 2020* underscores the importance of interoperability. As the Pentagon worked to hammer out a new vision statement for what the military should be capable of achieving around 2020, the underpinning of that vision was interoperability among the services. According to Marine Major General Henry Osman, the Joint Staff's director for operations, plans and joint force development, "Interoperability is the foundation upon which all of our doctrine and systems have to be based in order to achieve Joint Vision 2020.… The force must be fully joint, intellectually, operationally and technically ... not as a single military service, but rather the four services cooperating much more seamlessly."[25]

Ongoing work continues to support the importance of interoperability. For example, the 2001 Quadrennial Review (QDR), which is the most important evaluation effort the DOD engages in every four years, is expected to focus on information superiority and paticularly the interoperability aspect. Arthur Money, the Assistant Secretary of Defense for Command, Control, and Communications (ASD C3I), emphasized this in a recent statement:

> Indeed, information superiority may become the crux of the 2001 QDR. Money said defense officials will likely address two main subsets of information superiority—interoperability and information assurance—in the QDR, focusing on speeding up the time it takes for commanders to obtain accurate information and make a decision.[26]

In a talk on recent Army QDR efforts, to Harvard University's John F. Kennedy School, Brigadier General Lynn Hartsell echoed this position, highlighting feedback from the CINCs and the Army's Major Commands (MAJCOMs) that "Joint interoperability (especially C4ISR) is increasing important."[27]

3.2.3 Warfighter/CINC Emphasis

The CINCs, whom the Goldwater-Nichols Act considers the warfighters and who therefore possess tremendous power over the focus of DOD efforts, recognize that interoperability is fundamental. For example, the CINC for U.S. Space Command and Commander of Air Force Space Command, General Ralph E. Eberhart, who is responsible for supporting all the regional, geographic, and other specified CINCs, recently underscored the importance of interoperability in his USAF Leader Policy Statement, "North American Defense (NORAD) today has some 25 computer systems, almost as many computer languages, and more than two million lines of

---

[25] Hunter Keeter, "Joint Vision 2020 Should Reflect Better Interoperability, Official Says," *Defense Daily*, October 13, 2000.

[26] "CIO Says Military Must Shift Focus To Information Superiority," *Inside the Pentagon*, November 30, 2000, 1. Arthur Money is the ASD/C3I and Pentagon Chief Information Officer.

[27] Brig Gen Lynn Hartsell, U.S. Army, Director, Army Quadrennial Defense Review Office, "The Army Quadrennial Defense Review," lecture, National Security Fellows, National Security Program, Harvard University, John F. Kennedy School of Government, February 6, 2001, slide 8.

software code to support. When you talk about reliability, maintainability, affordability, and you talk about interoperability, it is the real challenge."[28]

That the DOD recognized the need for having a warfighting CINC as the advocate for joint interoperability demonstrates the significance of interoperability. In naming the Atlantic Command (ACOM)—now Joint Forces Command (JFCOM)—the force "integrator," the 1999 Unified Command Plan (UCP) assigned the command specific responsibilities to ensure that systems are interoperable and to conduct joint exercises and training aimed at improving and ensuring interoperability. Since that time, JFCOM has been actively engaged in measures aimed at improving interoperability.

[28] Gen Ralph E. Eberhart, Commander, United States Space Command and Air Force Space Command, U.S. Air Force, USAF Leaders Policy Statements: Ryan, Peters, Eberhart, Lyles, Myers, Email from Capt Timothy Cole, HQ USAF/XPS, Subject: News Clips, February 6, 2001, 15.

Chapter Four: Contributing Factors

Despite long-standing existence of DOD policy on interoperability and a process for interoperability certification, interoperability problems persist. A report on the 1999 Operation Allied Force (Kosovo) cited numerous combined-interoperability problems.[6] A General Accounting Office (GAO) report identified weaknesses in the DOD's interoperability certification process. The Commanders-in-Chief (CINCs) of the Unified Commands have frequently raised interoperability issues via the Joint Staff's Joint Warfighting Capability Assessment (JWCA) process, the CINC Interoperability Program Offices (CIPOs), and other fora.[1]

As asked in the introduction, how is it possible that after all the effort and money spent in the 15 years since the fiasco in Grenada there are still problems with interoperability in Kosovo? Why are CINCs and service staffs still concerned with interoperability?

It would be easy to fix the problem if a particular person, office, or institution could be identified as responsible. However, this just did not happen overnight and the people, offices, and institutions have all changed several times so that no single entity or person is to blame. Rather the answer is that combinations of factors contribute to the interoperability problem. These factors include the culture, dwindling budgets, rapidly changing technology, changing nature of operations, competing priorities, insufficient oversight, and unrealistic training and exercises. The result of these factors and their interaction create an environment that has hampered the accomplishment of interoperability over the past several decades.

4.1 The Culture

The first factor that affects interoperability is the culture in which the DOD acquires major weapons and automated information systems. Just looking at the number of organizations and people and the associated bureaucracy gives a glimpse of the challenge. There are three under secretaries or assistant secretaries of defense charged with oversight; at least two Joint Staff directorates responsible for review of requirements, oversight, and certification; a minimum of two CINC staffs--the originating CINC and JFCOM as the advocate of interoperability; the service staff responsible for procuring the system; and numerous defense agencies to include the Joint Technical Interoperability Center (JITC), which is responsible for testing and certifying the system as being interoperable. Add in the Congress and defense contractors and associated lobbyists and one can see the inefficiency in the process.

---

[6] Kosovo/Operation Allied Force, report in draft as of December 1999

[1] Jacques S. Gansler, USD AT&L, Arthur L. Money, ASD C3I, Philip E. Coyle, Director, OT&E, VADM S. A. Fry, Director, Joint Staff, memorandum for Secretaries of the Military Departments, USD for Policy, USD (Comptroller/Chief Financial Officer), ASD for Legislative Affairs, General Council, subject: Promulgation of DOD Policy For Assessment, Test, and Evaluation of Information Technology System Interoperability, December 4, 2000.

Ultimately no one is in charge of the process. Now, while this may be by design and for good reason, so as to thwart any overzealous person or organization, it still creates a culture or environment that factors into the efforts to achieve interoperability.

4.2 Dwindling Budgets

The dwindling budgets constitute another factor. The DOD budget has fallen over the past decade to the lowest percentage of Gross National Product in history. At the same time the demand for information faster has resulted in an increasing percentage of the budget being spent on information systems. According to Secretary Arthur Money, also the Pentagon's Chief Information Officer,

> He estimates the department is already spending anywhere from $75 billion to $100 billion a year on information technology—an estimation he said is nearly impossible to prove because so much of it is embedded within weapon systems and other defense programs. Providing resources to any of these activities, he said, is merely a 'balancing act.'[2]

However, according to Ms. Cheryl Roby, the Deputy Assistant Secretary of Defense for Command, Control and Communications, Programs and Evaluations, the portion that is tracked amounts to over 30 percent of the Secretary of Defense's budget.[3] This sets the stage for fierce competition between major weapons systems and automated information systems. Additionally, within information systems the limited dollars create greater competition between interoperability and capability, such as more bandwidth or faster processors, or functionality such as increased security.

[2] "Pentagon CIO Says Military Must Shift Focus To Information Superiority," *Inside The Pentagon*, November 30, 2000, P 1. Arthur Money is the ASD/C3I and Pentagon Chief Information Officer.

[3] Cheryl Roby, Deputy Assistant Secretary of Defense for Command, Control, and Communications, Programs and Evaluations, lecture, Command, Control, and Intelligence Seminar, John F. Kennedy School of Government, Harvard University, Cambridge, Mass., March 15, 2001.

4.3 Rapidly Changing Technology

> *Gordon Moore, a founder of Intel Corporation, observed in 1965 that the trend in the fabrication of solid state devices was for the dimensions of transistors to shrink by a factor of two every 18 months. Put simply, electronics doubles its power for a given cost every year and a half.*
>
> *In the three decades after Moore made his observation, the industry followed his prediction almost exactly. ... Moore's law is not a "law" of the physical world. It is merely an observation of industry behavior, It says that things in electronics get better, that they get better exponentially, and that this happens very fast.*[4]

The first factor that has significantly hampered accomplishing interoperability is the rapid rate of the change in technology over the past four decades. Using Moore's Law, as quoted above, one can extrapolate that, since Grenada, electronics have become over 1000 times more effective than they were then. More important, by 2016 (four years shy of the planned realization of *Joint Vision 2020*), electronics may be 1000 times more effective than they are now. It is easy to see the difficulties this poses for interoperability, given the unpredictability of what capabilities will be available even two years in the future, and the related problem of creating a new generation of systems every year and a half. This poses enormous challenges in terms of high expectations, creating legacy systems, and the ability to develop and apply standards to ensure interoperability.

4.3.1 Legacy Systems

> *The legacy systems issue is one of the greatest challenges faced by the DOD today.*[5]

Another product of the rapid change is technology is an increasing percentage of older generation legacy systems. As the generations of technology succeed each other at an accelerated pace, the new systems procured must interface with the older legacy systems. It is financially and organizationally impossible for DOD (or private industry, for that matter) to replace all of its computing systems, and the associated training and procedures, from the ground up every 18 months. It is equally unrealistic for the U.S. armed services to ignore the potential advantages offered by the latest technologies, especially when potential adversaries have access to them. Therefore, real-world demands dictate that the military strike a balance between replacing all of

---

[4] Robert W. Lucky, Understanding Computers and Communications, cited by The Information Resources Handbook, edited by Compaine and Read, MIT Press, Cambridge, Massachusetts, 1999, 87.

[5] Realizing the Potential of C4I, Chapter 4, 19-20.

its systems and "making do" by acquiring some number of new systems and devising ways to connect them with older generations of machines.

The NRC report highlights the prevalence and seriousness of this problem.

> The military services have tended to retain legacy information systems that were developed in response to "stand-alone" requirements, were not regarded as subject to connection with other systems and, therefore, are not operationally friendly with their increasingly interdependent companion systems. The legacy systems issue is one of the greatest challenges faced by the DOD today. This base of information systems comprises thousands of multi-generation electronic system elements and billions of dollars of capital investment, and is kept alive through the expenditure of many more billions in support costs. In the commercial world, such legacy systems are often kept operational based on a view their cost must be amortized before new capability can be economically justified. The military environment likewise seeks to amortize its investment; but the reasons are both functional and economic: the large-scale modernization of legacy systems entails major changes in training, doctrine, and organization, in addition to the difficulty of securing political support for new investment dollars. [6]

An example is when the DOD replaced the Secure Terminal Instrument, secure telephone, second generation system (STU-II) with the next-generation STU-III they were not interoperable, which meant that both systems had to be maintained until the STU-II was phased out years later. Realistically, legacy systems will remain a "fact of life" for the military, and will continue to plague interoperability. Recognizing this, DOD must seek ways to achieve the maximum interoperability attainable. One of the ways that they have attempted to do this is through establishing common interface standards for systems

4.3.2 Standards

> *…the interoperability problem has proven too complex to be dealt with by means of a single standard..*[7]
>
> *Interoperability remains a problem for commercial information technology…*[8]

---

[6] Realizing the Potential of C4I, Chapter 4, 19-20.

[7] Victor A. DeMarines, "Exploiting the Internet Revolution," in Carter, Ashton B. and White, John P., eds., *Keeping the Edge Managing Defense for the Future*, MIT Press, Cambridge, Mass., September 2000, 73.

[8] Realizing the Potential of C4I, Chapter 4, 21.

The challenge of establishing and implementing standards for interoperability when technology is rapidly changing is daunting. Many believe that simply defining standards for interoperability makes interoperability easy to achieve. On the surface it makes sense: If you define a technical parameter and all systems must comply with it, and then it follows that they should be interoperable. In fact, this is much more difficult than it seems because as technology changes then so naturally do the standards. Given the complexity of systems and the constant push to acquire the latest technology the challenge of ensuring standards for interfacing the new with the old or even the new with the new are tremendous.

DOD's effort to create a single integrated air picture (SIAP) serves as a good example of the technical difficulty associated with specifying standards for interoperability. In 1994, the ASD C3I promulgated a standard called "Link 16" and directed the services to implement it, but so far the interoperability problem has proven too complex for a single standard. At present it consists of several hundred pages of detailed technical information that requires interpretation and technical judgments. With no organization or mechanism to coordinate the judgments made by the many different programs implementing the Link 16, different systems comply with the standard different ways and cannot exchange data well enough to achieve a SIAP.[9]

This problem doesn't just exist with complex systems like those associated with Link 16. Another, more simple example is the different e-mail programs used by the services. All the services can interface from in-garrison when connected to their local server that is in turn connected to the World Wide Web. However, when they deploy with the same e-mail program they use in garrison and arrive at the deployed location and try to connect to the locally provided server that uses a different suite or program it doesn't work. As the systems become technically more complex, the difficulty of defining standards will also.

Another problem with establishing standards is the shift in industry in developing technology for the private sector rather than the military. Because DOD no longer enjoys the leverage it once had regarding the development and application of advanced information technology, the military must rely on commercial market technologies.[10] This dependence on commercial off-the-shelf (COTS) equipment, coupled with the streamlining of the DOD acquisition process to take advantage of the procurement of commercial items, complicates the process of establishing standards.

This is especially true when weapons must interoperate with command and control systems. Examples of attempts to set standards in this area are requirements that commercial items used in command and control and weapons systems conform to the Joint Technical Architecture (JTA) and the Defense Information Infrastructure/Common Operating Environment (DII/COE), which

[9] Victor A. DeMarines, 73.

[10] Realizing the Potential of C4I, Chapter 4, 38.

are sets of standards for interfaces and interoperability, before they can be purchased. However, when trying to apply these standards, many programs have found that the requirements to meet these standards severely constrain their choice and even terminology becomes a problem. For example, one program identified a problem with the data standards associated with the JTA, where less than ten percent of the relevant standards matched the data definitions employed in COTS items. [11] In response, the services added different interfaces that the COTS used to the architecture, therefore turning the JTA into a compilation of many different proprietary standards that did not interface with each other. As a result, a procured or acquired system could comply with the architecture, but still not be interoperable with other JTA compliant systems.

DOD's demand for "open systems" standards capable of interfacing with a myriad of manufacturers' systems is another sticking point for standards and a problem with commercial technology. The DOD values these open systems, where common interfaces instead of a proprietary ones are used, as the enabler for achieving that objective of interfacing multiple systems. Industry obviously wants to develop proprietary solutions to the demands of the market, and regards open systems as being an impediment with the protection of proprietary rights. In this vein, industry sees the DOD as wanting to own the intellectual property rights developed under government contracts so they can turn it over to a contractor's competitor in order to create a multi-source competition for potential procurements. "This is unacceptable to industry in a world where intellectual property is regarded as the most important factor for survival against highly agile, fast-moving competition."[12]

Lastly, standards are even more complicated when trying to ensure interoperability between U.S and multinational or coalition forces. Martha Maurer, an active-duty Air Force officer, in her research effort in Harvard University Program on Information Resources Policy provides insight into the task of ensuring interoperability between coalition forces:

> The level of effective interoperability between coalition forces will affect command and control. Prior efforts to achieve interoperability were primarily focused on making functional areas of combat interoperable between U.S. Services. If that goal is applied to coalition forces, it indicates a need for common standards and procedures across the board.[13]

---

[11] Discretionary-DOD Document, "Commercial Item Acquisition -- Considerations and Lessons Learned," Office of the Secretary of Defense, Washington D.C, June 26, 2000.

[12] Realizing the Potential of C4I, Chapter 4, 22.

[13] Martha K. Maurer, *Coalition Command and Control—Key Considerations,* National Defense University Press, Fort Lesley J. McNair, Washington, D.C.: July 1994, 97.

4.4 Changing Nature of Operations

Another factor over which DOD has little control over is the changing nature of warfare. As noted previously, the different military services historically conducted more or less autonomous operations. The concept of fighting jointly was codified in the Goldwater–Nichols Act of 1986 and has been further codified in joint doctrine and DOD directives. The trend toward multinational operations started with Desert Shield/Desert Storm in 1990/91, and reflects how we expect to conduct future operations.

These changes obviously bring with them challenges for interoperability—whether interoperability among U.S. forces or between U.S. forces and allied or coalition forces involved in multinational operations. Additionally, the changing nature of operations has altered the roles of various weapons systems and platforms, which also challenges interoperability.

4.4.1 Multinational Operations

> *Multiservice strike packages were difficult or impossible to assemble because various aircraft communicated in different ways over secure voice networks.*
>
> Les Aspin and William Dickinson[14]

As the quotation above highlights, problems of interoperability were prevalent between multinational forces even in Desert Shield/Desert Storm, which is considered an overwhelmingly successful campaign. *Joint Vision 2020* emphasizes that we expect to conduct operations not only as a joint U.S. force, but also with allied and coalition forces and international organizations. The lessons learned from Desert Shield/Desert Storm, the African operations of the 1990s, and the latest operation in Kosovo point out that the gap between U.S. technology and that of other countries causes an interoperability gap between the various allied forces.

Frank Snyder, a respected scholar on command and control, had this to say about multinational operations:

> The achievement of interoperability for combined operations in which the forces of friendly nations are organized to operate and fight together is even more difficult. The command and control of a combined operation requires resolution of all the issues that arise in a joint operation, but in addition, requires coping with national intelligence and sources, as well as considerations of national pride. The interoperability problems that can

[14]Les Aspin and William Dickinson, *Defense for a New Era, Lessons Learned of the Persian Gulf War*, in Frank M. Snyder, *Command and Control The Literature and Commentaries*, National Defense University Press, Fort Lesley J. McNair, Washington D. C., September 1993, 71.

> arise during combined operations with Third World nations may be very great indeed.[15]

The congressionally mandated National Research Council study of C4I programs highlights the technical aspect of interoperability and addresses the issues associated with multinational interoperability well. In addition to the differences in language, doctrine, and not knowing who our coalition partners may be, it identifies the following as factors that make it difficult or "essentially impossible" to achieve interoperability among multinational coalitions:

- Inadequate investments in and incompatible architectures
- National pride
- Individual nations information security requirements.

The study found that "Potential coalition partners, for the most part, lack adequate resources to modernize their C4I systems, and thus may well be using equipment that is substantially incompatible with present and planned U.S. C4I systems."[16] Also, because of national pride most nations favor indigenous military procurements of C4I systems, which reduces the likelihood that multinational systems will readily operate with U.S. systems.[17] Lastly, with regard to security of information the study highlighted that the United States places many restrictions on the types of information it is willing to share with certain coalition partners, which makes it difficult to develop interoperable information systems that allow only selective passage of information.[18] Multiply this same requirement by the number of nations involved and it becomes readily apparent that it is difficult to build interoperable systems.

4.4.2 Changes in Roles of Weapons Systems

With changes in technology and in the nature of war come changes in the roles of some weapons systems. For example, after the demise of the Soviet Union and the collapse of the Berlin Wall several platforms built to deal with the previous nuclear threat found themselves performing new functions. The B-1 bomber was assigned to a conventional role, which changed the nature of its communications and interoperability requirements from strategic to tactical.

When new uses for old systems are discovered then a corresponding change or addition of interfaces is required. For example, the discovery that the strategic warning system designed to detect and correlate a nuclear attack was capable of detecting launches of theater missiles resulted in an effort to provide warning at the tactical level. This significantly altered the requirements for

---

[15] Frank M. Snyder, 112.

[16] Realizing the Potential of C4I, Chapter 4, 13.

[17] Ibid.

[18] Ibid.

the communications systems, interfaces, and interoperability required for the warning systems to interface with theater tactical systems.

Another example of the change is the preference to use standoff smart weapons that require instantaneous or continuous communications between the weapons and numerous systems for command and control, guidance, and targeting information. The increased use of these weapons rather than more conventional platforms and the associated interface requirements create a numerous interoperability challenges.

Still another example is the increased demand for real-time intelligence and imagery so that the pilot in the cockpit or soldier in the foxhole has the latest imagery of the target or battlefield. This creates tremendous interoperability challenges. The list could go on almost indefinitely. In any case, it is safe to surmise that continuing changes in the nature of war will only increase the challenges for interoperability.

4.5 Priorities

The general principle that operational needs should drive the acquisition system is well established within DOD. Under current practices (i.e., the traditional acquisition system), warfighter input (based on the perspectives of the CINCs) is codified in terms of validated military requirements, which are vetted as the basis for new program starts. The acquisition system takes the military requirements and then—some years later—provides for fielding a system intended to meet those requirements.[19]

While DOD can only respond to the factors discussed in the previous sections, it can set and enforce priorities that promote acquisition of interoperable systems and help to achieve interoperability among existing systems. Without fixed--and enforced--procedures, organizations, systems, and functions will continue to clash over conflicting priorities among requirements and funds.

4.5.1 Service versus CINC Priorities

The problem is that while the Department of Defense assigns warfighter responsibilities to unified commands, each individual service is responsible for developing its own command and control systems…this creates some big, ugly seams for joint commanders.[20]

Hoot Gibson, Colonel, U.S. Air Force Director of the Commander–in-Chiefs Interoperability Program Office

[19] Realizing the Potential of C4I, Chapter 4, 43.

[20] "Office makes all pieces of the puzzle fit together," *Hansconian,* Electronic Systems Command, Hanscom Air Force Base, Mass., September 22, 2000, 3.

The experience of the U.S. Special Operations Command (SOCOM) offers a useful lesson:

> …as no surprise, a high degree of C2 interoperability and effectiveness is achievable if an organization is guided by joint priorities. Whereas the services procuring C2 systems for mainstream forces usually have other, higher priorities than interoperability with the other services or interoperability with all of the regional commands, SOCOM's priorities have been driven by its structure as a joint organization, and its recognition that it must retain the political support of the regional CINCs to survive.[21]

SOCOM enjoys the unique luxury of having its own funding line and being able to procure its own systems. The other unified and specified commands do not have that luxury and must depend on the service components to procure or acquire their systems. As a result, the different perspectives of the services and the CINCs immediately create problems with interoperability and competing priorities.

Under current guidelines and public law, requirements are identified by the warfighting CINCs and then codified and acquired or procured by the services, which have the responsibility under United States Code (USC) Title 10 to "equip the forces " with systems to support the warfighting CINCs. Victor DeMarines, former president of The MITRE Corporation, describes the problem plaguing joint C2 as "the difficulty of achieving horizontal integration in vertically funded world…"[22]

Most criticism is leveled at the services, saying that their perspectives and priorities do not match those of the CINCs or warfighters. The CINCs argue that:

> Warfighter input (especially that from a joint perspective) can be diluted when individual services are responsible for the articulation of system performance requirements and specifications. The reason is that while the initial specification of requirements may indeed be joint and operationally based, all development projects entail further refinement of specifications as they proceed (this is especially true if a spiral development process is used). A service perspective—rather than a joint one—is thus automatically present as such refinement proceeds. For C4I systems that are primarily of interest to one service, such a perspective will probably enhance the outcome. But if the system is primarily of interest to a joint commander, or if the system is likely to depend on data provided by C4I systems in other services, a service perspective may well detract from (joint) interoperability and/or full functionality.[23]

---

[21] Victor A. DeMarines, 75.

[22] Ibid, 77.

[23] Realizing the Potential of C4I, Chapter 4, 43-44.

Such critiques, which tend to focus on issues related to "turf," no doubt capture a major reason for the friction between services and joint commanders, but in some cases place unfair blame on the service components. Part of the problem is that a service often does not know how the system is to be operationally deployed—a problem related to the volatility of the world situation and to the ongoing changes in the nature of warfare, as previously discussed. The result is that a service produces an Operational Requirements Document that does not capture what the system must do or must be interoperable with. By the time joint commanders review a proposed system, it may be too late to make major changes.

Also complicating the issue is that the different regional CINCs have differing requirements, which presents a major problem for interoperability. This is demonstrated on a microlevel with the challenges that SOCOM faces in supporting the regional CINCs. "SOCOM has from its inception placed a very high priority on understanding the needs of the regional CINCs who actually employ the Special Forces that SOCOM trains and equips. This has led to a heavy emphasis on making C2 systems fully interoperable with those of the CINCs, even at the expense of standardization. For example, a special operations unit that moves from the Pacific Command to the European Command may require two full days to modify its organic C2 systems."[24]

Lastly, another area of contention is the timeframe of focus. The CINCs' primary focus is on fighting today's war, so they do not look as much toward future requirements. By contrast, the services continually look ahead in order to plan, program, and budget to replace current force structure; they are by nature more visionary. While this can cause conflict with a CINC who wants the services to meet a requirement for today's war, it is understandable why, in an environment with limited funds, a service may trade off today's requirement to meet tomorrow's needs.

4.5.2 C4I versus Weapons Systems Priorities

> *... the appropriate balance between weapons systems and C4I technology will continue to shift, posing major challenges for the military services.*[25]

Command and control systems do not yet fit neatly into DOD's acquisition system. According to General William F. Kernan, the new CINC of JFCOM, "Most defense acquisition budget is focused on large-scale systems such as vehicles, ships, and aircraft. But the military's command, control, communications, and computer capabilities are essential to synchronous operations…"[26] The congressionally mandated study by the National Research Council draws

[24]Victor A. DeMarines, 75.

[25] Realizing the Potential of C4I, Chapter 4, 8.

[26] William H. McMichael, "Uncertainty, challenges await Kernan," *Air Force Times*, February 12, 2001, 16.

similar conclusions: "The organization, procedures, and regulations governing acquisition of military capabilities are oriented largely toward major weapon systems for which the time from concept definition to fielding of the first article of production typically ranges from 10 to 15 years."[27] C4I systems must compete in the service budgets with hardware that the services are obligated to provide under the terms of the National Security Act. "Those rules are built so that DOD spends most of its dollars on ships, tanks, and airplanes; they don't fit command and control systems very well."[28]

This is not a new phenomenon. William Odom, former military assistant to the President's assistant for national security affairs, described the environment well in a 1980 lecture at Harvard University's John F. Kennedy School of Government:

> *Who do you think pays for the JCS and the CINCs and the President's command and control—or, to put it colloquially, their telephone bill? The military services [do]. And this creates enormous budgetary and political strain with the Defense Department. If the Air Force has a choice between buying more airplanes or providing a command and control plane for the President, and providing more radios and ADP capability for control of the center of the JCS, they prefer to buy airplanes, not the control. The Army prefers tanks to paying for the President's White House communications system. The Navy has its preferences along the same lines.*[29]

In terms of funding, decreases in the DOD budget over the past two decades require that the department get the most out of limited dollars. Usually, this has meant that if DOD must choose between capability and interoperability, capability wins out.[30]

4.5.3 Interoperability versus Performance Priorities

> *… unlikely to change the priorities of the individual system program offices, which tend to assign the highest priority to functionality, the second to interoperability with other systems of the same service, and the third to joint interoperability.*[31]

---

[27] Realizing the Potential of C4I, Chapter 4, 15.

[28] Less Paschall, Consultant; former Director Defense Communications Agency and Manager Defense Communications System, "C3I and the National Military Command System" (1980, pp. 67-86), in Thomas P. Coakley, *C3I: Issues of Command and Control*, National Defense University Press, Fort Lesley P. McNair, Washington D.C., 171.

[29] William Odom, "C3I and Telecommunications at the Policy Level," in Thomas P. Coakley, *C3I: Issues of Command and Control* (1980, pp. 1-23), National Defense University Press, Fort Lesley P. McNair, Washington D.C., 169.

[30] Realizing the Potential of C4I, Chapter 4, 8.

[31] Victor A. DeMarines, 74.

The experience of several decades suggests that the critical decisions will be the engineering trade-offs necessarily made in the course of developing or modernizing any state-of-the-art system. At any given moment in time, the constraints of technology, budget, and schedule always require that some performance objective be compromised in order to achieve others.

The program manager who is in charge of acquiring a particular system is graded on the three items of cost, schedule, and performance. The cost is considered the fixed variable, which leaves schedule and performance as the trade-offs.

One manifestation of these pressures is the importance of reprioritization in light of trade-offs between interoperability or security. This can lead to significant reductions in interoperability or security in order to meet schedule and budget commitments.

4.6 Oversight

> *... I think all he [the Secretary of Defense] has to do is saddle up somebody in OSD and give him the clout to enforce interservice integration [integration here refers to interoperability of communications equipment "owned" by different Services].*
>
> Robert T. Marsh
> Commander, Air Force Systems Command[32]

DOD also has control over the degree of oversight it exercises: the second area that must be improved if interoperability is to be achieved. After establishing the priorities and codifying them in policy and guidance, DOD must enforce the directives if it is to achieve its goals. Oversight includes ensuring that the systems are tested, evaluated, and certified as interoperable. DOD has issued new directives aimed at codifying the process for ensuring that interoperability requirements are included and that systems are tested and certified. However, it will take years to evaluate the impact of this guidance. In the meantime, the department must deal with the current problems, and if the initiatives fail these problems will continue to plague efforts to achieve interoperability. The specific areas that are of concern are the different oversight requirements associated with different acquisition categories, ineffective or ignored directives, and the failure of organizations to comply with interoperability certification.

[32] Robert T. Marsh, former Commander Air Force Systems Command, "Air Force C3I Systems," in Thomas P. Coakley, *C3I: Issues of Command and Control*, National Defense University Press, Fort Lesley P. McNair, Washington D.C., 227.

4.6.1 Level of Information Systems Programs

Different levels of acquisition programs are based on dollar thresholds and importance, and receive correspondingly different levels of oversight. This is important because the majority—an estimated 80 percent—of information systems fall in acquisition category 3 (ACAT 3), which receives less oversight than the category 1s or 2s. Therefore, the oversight to ensure interoperability requirements are met for the majority of systems falls to the services, rather than of OSD. "The service acquisition executives must ensure that ACAT2/3 programs meet Joint Interoperability requirements, since the programs (and to a lesser extent ACAT 1C) typically do not get close scrutiny at the OSD level."[33] The remaining 20 percent meet the dollar threshold to be in category 1 or are important enough for their requirements to be vetted through the Joint Requirements Oversight Council, the Defense Acquisition Board, or the Major Automated Information Systems Review Council. However, this does not necessarily solve the problem, because these bodies perform a review and oversight function for many programs. This means that they are limited in the attention that they can give to any specific program.[34]

4.6.2 Enforcement of Directives

The second area where oversight needs to be improved to ensure interoperability is in the enforcement of directives. A 1998 report by the DOD inspector general highlights this issue, saying that "… directives intended to assure jointness and interoperability of C4I systems have proven relatively ineffective because program managers and the services have few institutional incentives to comply with them, and few penalties accrue to C4I programs that are not interoperable."[35]

As noted previously**,** few commercial products initially met the standards established for the JTA, which resulted in additions that only complicated system interfaces in the standard. Despite a directive by the ASD C3I that made the JTA mandatory for all C4I systems, the inspector general's report found non-compliance in the plans of many C4I programs. If such non-compliance appears in a program's written plans, one can only assume that even though some others have written compliance into their plans, they will not in fact comply.[36]

The DOD offices responsible for oversight argue that they lack the authority to enforce compliance because they do not control the money that is the "carrot or stick" for the services and agencies. However, the report placed the major blame on the overall process, emphasizing that:

---

[33] RADM R.M. Nutwell, U.S. Navy, Deputy Assistant Secretary of Defense for C3ISR/S, "Achieving Joint Information Interoperability," Version 1, April 4, 2000, 14-15.

[34] Realizing the Potential of C4I, Chapter 4, 54.

[35] Ibid, 12.

[36] Ibid.

> While certain C4I oversight offices within DOD do have the ability to withhold budget authority from the services for C4I programs that are not paying sufficient attention to C4I interoperability" because they "do not in general have budgets of their own to spend on efforts to promote interoperability…stopping programs that do not comply with requirements for interoperability requires identifying them in the first place, and then investing time and political capital—a highly inefficient process.[37]

As a result, according to the National Research Council report, "… the behavior of program directors and managers has evolved little—nor has that of an oversight process established to ensure that every acquisition of significance satisfies the traditional acquisition regulations."[38]

4.6.3 Certification of Information Systems

The last component of oversight that warrants discussion is certification of compliance. The services and agencies have tended to ignore the standing requirements for systems to be certified by the Joint Interoperability Test Center (JITC). The current JITC commander has stated that the services or agencies simply do not bring their systems to the JITC for testing and certification.[39]

A 1998 General Accounting Office (GAO) report reveals the magnitude of the problem. The GAO found that the CINCs, services, and agencies were not complying with the C4I certification requirements. Their findings included that a significant number were not submitted for testing, so that testing covered no newly developed systems under the C2 initiatives program and none of the systems under the advanced concept technology demonstration program within the past 3 years. Also, the GAO found that there was no consistency with regard to re-certifying modified systems. Lastly the GAO charged that the JITC was not advising the services of interoperability problems identified in exercises, even when they could have resulted in loss of equipment, supplies, or even lives.[40]

DOD has issued new directives requiring JITC certification before a system is allowed to go into production. However, it remains to be seen if the services will comply with them. The JITC is a fee for service organization, which means that the services have to pay to have the systems certified. This may help explain some of the reluctance. However, based on the track record and reluctance exhibited so far and lack of enforcement of the requirements, compliance may well be spotty or slow to come.

---

[37] Realizing the Potential of C4I, Chapter 4, 12.

[38] Ibid, 37.

[39] Colonel Ben Osler, USAF, Commander, Joint Interoperability Test Center, telephone interview with author, October 2000.

[40] General Accounting Office 1998, Joint Military Operations: Weaknesses in DOD's Process for Certifying C4I Systems' Interoperability, Report No. NSIAD-98-73, General Accounting Office, Washington D.C., cited in: Realizing the Potential of C4I, Appendix B, 21.

4.7 More Frequent and Realistic Training/Exercises

The last factor discussed, over which the DoD has control, is training. Vice Admiral S. R. Arthur, Commander of Navy Central during Desert Storm, highlighted in the Navy's lessons learned the need to focus on interoperability, saying, "[w]hen deployed, joint and multinational operations/exercises should focus on interoperability issues—comms [communications], tactics, limitations."[41]

Training provides the opportunity to train personnel as well as identify equipment and system interoperability shortfalls so they can be fixed. More important is that training should be conducted so that it provides realistic learning and assessments of both personnel and equipment so that remedial or corrective actions can be taken to overcome deficiencies. The bottom line is that equipment and people should be exercised frequently and in a realistic environment.

This is not a new phenomenon. Robert R. Everett, former president of The MITRE Corporation, in a 1981 address to Harvard University's C3I seminar, when replying to questions about if the German and French postal, telephone and telegraph systems can work together why can't the U.S. Army talk to the U.S. Navy , said it well:

> Now as it turns out, the German and the French PTTs will work together; the French and the Germans do talk to each other, and that has been true ever since the early days. Therefore, in the course of evolution, it's worked. But if they had never talked to each other and a time comes, at two o'clock in the morning, when they will need to talk together, rest assured they won't be able to. This is the situation in our military. People say, 'It's just absurd that the Army and the Navy can't talk to each other. We'll legislate it: Everybody shall buy the same radios; or, we'll make them get together in one room and design the communications center.' Those things don't work. The only way you're going to get them to work together is to make them work together, make them work joint exercises, and when they can't work together and the thing fails, you sneer at them and they have to go out and fix it. If you don't do that, they won't ever fix it.[42]

He hit it the nail on the head: the key to ensuring that the people and systems working together lies in joint training. This means that training must be conducted frequently to ensure maximum readiness. However, as it stands now most of the training is conducted at the individual services' unit levels, not jointly. The services also have the responsibility for training the forces, so a major component of training is unit exercise. Because unit training is more prevalent with

---

[41] U.S. Navy in Desert Shield/Desert Storm, VI: Lessons Learned and Summary, Department of the Navy, Naval Historical Center, Washington D.C., 1. Quick Look –First Impressions Report, March 22, 1991.

[42] Robert R. Everett, President MITRE, in Thomas P. Coakley, Ed., *C3I: Issues of Command and Control*, National Defense University Press, Fort Lesley J. McNair, Washington D. C., 1991, 185.

other units and systems from the same service, interoperability problems within the services are more likely to be identified and fixed to maximize intra-service operations. However, by contrast, joint exercises and training are relatively infrequent and involve a set of variable systems interactions among the units that happen to train together. Even when problems are identified the immediate pressure to fix problems arising in a joint context is considerably less because the unit will not exercise with the other unit for a long time (if ever again) as compared to the pressure to fix problems that arise in same-service unit exercises, which are more frequent and subject to greater scrutiny. Local incentives are thus missing from joint exercises and many interoperability problems may remain hidden because the systems are not exercised often or thoroughly enough.[43]

Equally important is the frequency of training and exercises. More frequent exercises are required to evaluate and ensure readiness of people to operate in joint operations. Again, because of the infrequency of opportunities to participate in joint exercises people are not exposed to realistic conditions or trained as they are expected to fight. Take for instance Cobra Gold, conducted annually in Thailand. Because the Joint Task Force Headquarters rotates between the U.S. Army First Corps and the U.S. Marines Third Marine Expeditionary Force each year, the Air Force unit that provides communications support for the Air Operations Center only gets to exercise with each of the JTF Headquarters biannually. Add in the rotation of personnel and it means a significant percentage of people deploying to the area for the first time. Ensuring effective training and evaluation of the people requires more frequent training.

The second issue associated with joint training is that it must be realistic. Often this is not the case as exercises are usually designed to maximize operational objectives and do not realistically exercise deployment or employment of communications systems. The usual scenario is that the communications people deploy well in advance of the operators and set up the communications systems and networks. During the course of the exercises communications outages or problems are simulated so as not to risk a real outage that might jeopardize achieving the operational goals. Again, this is not a new concept; in fact it was one of the lessons learned highlighted by Admiral McDonald, CINC of Atlantic Command, in response to questioning during his testimony in congressional hearings on the Grenada operation:

> We do conduct communications exercises in the Navy, but in these exercises, we give our communications about 12 months preparation. Therefore, it should not be surprising that when the exercises start, communications work…. Our failure in preparatory exercises to uncover and anticipate problems similar to those we faced in Grenada may have been because our exercises are over prepared. Given enough time, anyone can make communications work. Unfortunately, in a crisis situation—a 'come-as-you-are' situation—they do not work.[44]

---

[43] Realizing the Potential of C4I, Chapter 4, 11.

[44] Colonel Stephen Anno and Lieutenant Colonel Willaim E. Einspahr, *Command and Control Lessons Learned:*

Part of the problem may be that Desert Storm reinforced that realistic training for deploying and employing communications is not necessary because we had over 6 months to set up and establish communications. So in our usual manner of fighting the last war, and despite the need for realistic training being highlighted 20 years ago, the norm during exercises is still for the communications personnel and equipment to deploy early and establish communications ahead of the arrival of the operators. In the Cobra Gold exercises, it is common for the people and equipment to arrive in Thailand 2 weeks to a month prior to the actual start of the exercise and even then there are still problems when the operators arrive. This fails to exercise realistically the concept of rapid deployment and the philosophy of "come as you are."

Another area that impacts realism is simulation. Often duplicate systems are built to simulate real-world systems and to keep exercise communications separate from real-world communications. However, these systems are often incapable of directly duplicating real-world operational C4I systems. The surrogate systems created to carry out the exercises lack the true similarities of the real-world systems, and thus fail to provide adequate training and to uncover interoperability problems.[45] This denies both the operational and communications personnel realistic training. A second part of simulations is that to maximize operational training communications failure scenarios are usually simulated so that the systems are actually not taken off line to realistically demonstrate the lack of capability. Martha Maurer, a pioneer in coalition research and author of a widely praised book on coalition warfare, highlights this and that many exercises have a primary operational orientation where unknowns or less important concerns, such as C3 availability, are assumed away. She emphasizes that ways are needed to test command and control systems as if in war or in absolute reality. Otherwise the systems are not effectively evaluated.[46] So the problem is twofold, in that the exercises need to use the real systems that will be employed in the real world, and scenarios designed to exercise communications outages or degrades need actually to take the systems off line instead of simulating them away. Without these conditions, both operational and communications people will not be effectively evaluated and the opportunity to improve operations or fix problems missed.

While all of these experts stress the dichotomy between what exercises are officially meant to achieve and what the participants actually seek to achieve, there is proof that exercises have contributed to real-world successes. Take the U.S. Navy's experience in Desert Shield/Desert Storm and the practical effectiveness of SOCOM. The Navy attributes much of its success in the Persian Gulf War to appropriate exercises, where years of close cooperation and coordination

---

Iranian Rescue, Falklands Conflict, Grenada Invasion, Libya Raid, Chapter IV, "The Grenada Invasion", Air War College Research Report, No. AU-AWC-88-043, Air University, Maxwell Air Force Base, Alabama, [reprinted as an extract from by The United States Naval War College Operations Department, NWC 2082, http://www.fas.org/man/dod-101/ops/urgent_fury.htm], accessed last on February 5, 2001, 43.

[45] Realizing the Potential of C4I, Chapter 4, 63.

[46] Martha K. Maurer, *Coalition Command and Control*, National Defense University, Fort McNair, Washington, D.C., July 1994, 105.

with the navies of our NATO allies and other coalition partners in regular bi- and multi-lateral exercises and during the Iran-Iraq war laid a strong foundation of interoperability and common procedures.[47]

While never wishing to place people in harm's way, ideally C2 systems would be tested in real-world settings such as those experienced by SOCOM, which attributes much of its successes to real-world experience, citing that SOCOM's forces have frequently been involved in real operations against real enemies. Because of their uniqueness and frequent involvement in real world operations, SOCOM's C2 systems are frequently tested in operational conditions, thereby ensuring that any failures of C2 interoperability will be noticed and remedied on an urgent basis.[48] For the rest of the military this opportunity does not exist, so the only way to train and evaluate personnel and systems is through realistic exercises and training.

In summary of training, efforts are required to ensure that exercises and training are realistic and timely. The frequency of training must be increased to ensure that the people are trained and equipment maintained at peak performance. The exercises must be more realistic. Equipment and personnel must be deployed and employed during exercises as expected, not weeks or a month ahead of the arrival of the operators. Also, simulations should be minimized and where necessary must be as realistic as possible to mirror real-world operations in order to evaluate personnel and identify equipment problems so they can be fixed.

[47] U.S. Navy In Desert Shield/Desert Storm, 1.

[48] Victor A. DeMarines, 75.

Chapter Five: Mitigating Initiatives

There are many Joint Interoperability initiatives underway addressing several fronts: policy, requirements, acquisition, resources, process, and procedure. Coordination of these varied activities is difficult at best. Cost is high and the actual result of these efforts is yet to be determined.[1]

While it is impossible to predict what will happen in the future there are several recent changes to policy and guidance, organizational roles, and the acquisition process that are aimed at mitigating the effect of the factors addressed in the previous chapter and at ensuring interoperability. Although it will take several years to implement these changes and even longer to determine their overall success, they will definitely impact future interoperability and if these efforts reach their goals the prospects of interservice interoperability almost certainly will improve.

5.1 New Policy and Guidance

Three related policy and guidance documents, updated and implemented over the past 18 months, contain significant changes, that make interoperability a priority and hold potential for improving interoperability among the services. These documents are the DOD Instructions (DODIs) 5000 series, which governs the acquisition process; and two Chairman of the Joint Chiefs of Staff Instructions (CJCSIs), the first of which mandates procedures for the requirements generation process and the second of which addresses interoperability and support to national security systems and information technology systems.

The first of the related group, signed into effect August 10, 1999, is CJCSI 3130.01A, *Requirements Generation System.* It sets policy for the CINCs, services, and agencies regarding how requirements are identified and systems acquired to meet the requirements. The document contains three major changes related to interoperability that bear discussion. Two of the three--time-phased requirements in support of evolutionary acquisition and the roles of JFCOM--will be discussed under the following topics of acquisition initiatives and organizational changes respectively. The third change is associated with key performance parameters (KPPs). CJCSI 3130.01A establishes a first by mandating that Interoperability KPPs be included in requirements documents and mission need statements, the two most critical documents in the acquisition system, for major automated information system acquisition programs.[2] Including interoperability in the KPPs that an acquisition program must meet before it can proceed to the next phase of the

---

[1] Paul D. Szaboados, Office of the Deputy Assistant Secretary of Defense for Command, Control, Communications, Intelligence, Surveillance, Reconnaissance, and Support/Program, Analysis, and Integration, issue paper, subject: Joint Information Interoperability Initiatives 2000, undated.

[2] Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01A, *Requirements Generation System*, August 10, 1999, 3.

acquisition cycle (e.g., concept exploration, component advanced development, system development and demonstration, production and development, etc.) means that programs must meet systems interoperability requirements by the end of each phase prior to advancing to the next.

CJCSI 6212.01B, signed into policy May 8, 2000, aligns itself with 3170.01A by building on the methodology to help ensure interoperability. The document describes a methodology for developing interoperability KPPs and links them to a set of Information Exchange Requirements (IERs),[3] defined as information exchanges between CINC, service, agency, and coalition systems. In layman's terms, an IER, "…identifies who exchanges what information with whom, why the information is necessary, and how the information must occur."[4] This is important and a breakthrough because where previously performance was tied to a vague standard such as the JTA or DII/COE, it is now defined in relation to which systems from within the service and among other services the systems must operate with. Additionally, CJCSI 6212.01B also establishes the minimum threshold and objective criterion for accomplishment of KPPs before an acquisition program is allowed to proceed to the next milestone, there making interoperability a "showstopper" for the first time. The threshold criteria, which are the minimum IERs a system must satisfy, are now typically defined as all or 100 percent of the critical IERs, with the objective criteria being the accomplishment of all the rest of the IERs.

Lastly, the CJCSI puts in place a mechanism for the Joint Staff's J-6 validation process requiring the J-6 review of requirements and certification documents to ensure that the interoperability key performance parameters are met for all systems. This J-6 validation is intended to provide total life-cycle oversight of warfighter interoperability requirements. In validating a system the J-6 validates that the interoperability KPPs derived from the set of IERs approved in the requirements documents and C4I support plan were adequately tested and testing results certified.[5]

The last of the group of inter-related documents, which was signed into effect January 4, 2001, are the DODIs. DODI 5000-2 reiterates that all information technology acquisition programs developed for U.S. forces must be for joint, combined, and coalition use, or in words commonly used by Pentagon action officers must be "born joint."[6] The DODI also strengthened the prospects for achieving interoperability by expanding the policy established by the two

---

[3] Briefing, Commander Mark Genung, U.S. Navy, Joint Staff/J6I, subject: CJCSI 3170.01A "Requirements Generation System" and CJCSI 6112.01B "Interoperability and Supportability of National Security Systems, and Information Technology Systems," January 16, 2001, slide 8.

[4] Ibid, slide 7.

[5] Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6112.01B, *Interoperability and Supportability of National Security Systems, and Information Technology Systems*, August 10, 1999, 4.

[6] Department of Defense Instruction (DODI) 5000.2, *Operation of the Defense Acquisition System (Including Change 1)*, January 4, 2001, 11.

referenced CJCSIs to all acquisition categories so that, "The Chairman of the Joint Chiefs of Staff shall establish procedures for the development, coordination, review, and validation of interoperability and supportability of IT (including NSS [National Security Systems]) acquisition programs, regardless of acquisition category."[7] This is a major change aimed at overcoming oversight problems associated with those lower category programs (see section **4.6**).

5.2 Organizational Changes

As noted in section **3.2.3**, the path to organizational evolution and responsibility began in 1993 with assigning U. S. Atlantic Command, now JFCOM, responsibility for training and providing CONUS-based forces to support the needs and operations of the regional CINCs. When ACOM was re-chartered as the JFCOM in October 1998 it was given a broad set of responsibilities for supporting joint operations, to include being the Joint Force Integrator. The provisions of the UCP, which assigns responsibilities to the CINCs, provided JFCOM with a mandate to promote jointness and chartered its involvement in the joint requirements process.[8] CJCSI 3170.01A codified the command's role for interoperability. In another first, it assigned responsibility to act as the advocate for interoperability, "USCINCACOM will serve as the Chairman's advocate for joint warfighting interoperability. USACOM will provide the warfighter perspective during the development of joint operational concepts to ensure that joint forces have interoperable systems."[9]

As a result, now JFCOM has the opportunity to participate on every level of decision making from the integration process team to CINC involvement in the requirements oversight process to the Defense Acquisition Board that oversees and approves the acquisition of major weapons and automated information systems.[10] "Accordingly, the command has begun to advocate jointness and interoperability in generating requirements which provides opportunities to influence the development and approval of all mission needs statements regardless of acquisition category or origination source and the staffing of service-generated operational requirements that is critical because these documents define program performance parameters for improving interoperability."[11]

Since inheriting its new mission, interoperability has been a key focus for JFCOM. A February 2001 interview with the new CINC for JFCOM, General William F. Kernan, highlighted the CINC's key role in ensuring interoperability, saying that most important is that, "If a system

---

[7] DODI 5000.2, 11.

[8] Victor A. DeMarines, 79.

[9] CJCSI 3170.01A, B-7.

[10] Harold W. Gehman, Jr., Admiral, US Navy, "Progress Report on Joint Experimentation, *Joint Forces Quarterly*, Summer 2000, http://www.dtic.mil/doctrine/jel/jfq_pubs/1325.pdf, accessed March 6, 2001, 82.

[11] Ibid.

does fill the interoperability requirements…Kernan can give it the boot."[12] While this may be debated the fact that an operational CINC has been designated to act as the advocate for interoperability and that the command is involved in the requirements and acquisition processes for all automated information systems carries tremendous potential toward ensuring interoperability.

Also, JFCOM plays a major role in training.

> With calls for improved interoperability among the services, the Joint Chiefs recommended that ACOM be assigned responsibility for joint training and integration. Changes in the Unified Command Plan directed that then ACOM assume peacetime control over U.S. Army Forces Command and Air Combat Command. Today, JFCOM is the provider, trainer, and integrator of joint forces.[13]

Having a CINC in charge of training and integrating joint forces and then assigning control of the CONUS forces to him provides the leverage for increased joint training.

Additionally, the October 1998 UCP assigned the ACOM responsibility for the DOD's Joint Experimentation Program aimed at exploring and validating future joint operations and concepts that will drive changes to doctrine, organization, training, and education, materiel, leadership, and people (known collectively as DOTMLP). With this role the command added a Joint Experimentation Directorate, J-9, in October 1998, which laid the foundations for "working with the services, unified commands, defense agencies, industry, and academe on exploring new concepts."[14] One of the keys to the experimentation program is that it does not rely solely on simulations, but combines simulation with real operational exercises. "Some good things can be done by computer driven modeling and simulation, but sooner or later, we must try new operational measures in the air, at sea, and on the ground."[15] For example, fleet exercises in the 1930s that defined carrier warfare to the Army's famous Louisiana Maneuvers of 1941 that developed combined arms air/ground operations the experimentation program relied on live war games.[16] JFCOM hopes to have similar results from its exercises such as the upcoming Millennium Challenge 2002 which is being designed to provide a venue to exercise service

---

[12] "Uncertainty, challenges await Kernan," *Air Force Times*, February 12, 2001, 16.

[13] Harold W. Gehman, Jr., Admiral, U.S. Navy, 78

[14] Ibid.

[15] Mission statement, US Joint Forces Command, subject: USJFCOM Command Mission, http://137.246.33.101/cmdmission1.htm, accessed March 3, 2001, 2.

[16] Ibid.

operational concepts and examine and identify strengths and weaknesses in interoperability and integration of service warfighting concepts in a joint environment.[17]

5.3 New Acquisition Process

Although we can't control the rate of change in technology, in an attempt to minimize the impact, the DOD adopted a new acquisition strategy.

> *The realization that the rate of change in technology as well as in operational requirements (especially in C4I) is not matched to the typical multiyear cycle time for traditional system acquisition has led to the concept of evolutionary acquisition, also known as "spiral development."*[18]

Given a validated requirement and an approved architectural framework for future development, evolutionary acquisition allows more rapid deployment of systems and provides a process for incremental upgrading of fielded systems. Conceptually, the requirements, definition, testing, and fielding steps of traditional acquisitions are executed over much shorter cycle times for each incremental deployment. Evolutionary acquisition permits incremental addition of capabilities to a system and the underlying technologies evolve without this being viewed as 'requirements creep.'

As mentioned earlier one of the three major things that the CJCSI 3170.01A did was related to the evolutionary acquisition approach. The CJCSI 3170.01A codified time-phased requirements in support of evolutionary acquisition aimed at a streamlined acquisition strategy that fields a core capability with a modular open structure and that provides for additional future increments in capability upgrades. The instruction states "Automated Information Systems are prime candidates for evolutionary acquisition"[19] which will help cope with and take advantage of rapidly changing and developing technology.

A fundamental tenet of evolutionary acquisition is acceptance of the "80 percent solution." Insistence on a "100 percent solution" can radically increase costs and extensively delay system deployment. It should be stipulated that an 80 percent solution is the goal for virtually all C4I acquisitions. The rationale is simple: no C4I system requirement can be effectively specified to the 100 percent level, nor can any C4I acquisition program deliver a "final" solution. An 80 percent solution allows the program design to take advantage of the inevitable changes in the underlying information technologies. It also provides a base of experience on which to specify

---

[17] Instructions for Joint Initiative Submission and Review Process for Millennium Challenge 2002, "Background,," http://137.247.242.50/Key%20Reports/Instructions%20v4%20-%20to%20CoS.doc, accessed March 3, 2001,p 1.

[18] Realizing the Potential for C4I, Chapter 4, 16.

[19] CJCSI 3170.01A, 3, E-2.

and build the remaining functionality. And, it allows a more gradual path for possible changes in doctrine and tactics for using the capabilities provided by a new C4I system."[20]

A prime example of successful 80 percent rule application is the Global Command and Control System (it is one of a very few major C4I acquisition success stories). The Global Command and Control System objective was functional: replacement of the antiquated World Wide Military Command and Control System with new, high-technology-based global C4I system capabilities--without sacrificing the essential capabilities of the legacy system.[21]

[20]Realizing the Potential of C4I, Chapter 4, 16-18.

[21] Ibid.

Chapter Six: Is It Really Achievable?

6.1 Recap

As asked at the beginning, how nearly 15 years after the fiasco in Grenada and the millions of dollars spent and tremendous efforts to fix interoperability problems did we still have interoperability problems in Kosovo? Why do CINCs of the unified and specified commands and service chiefs still raise issues associated with interoperability?

Lessons learned from Grenada through Kosovo show a continuing trend of problems with interoperability among U.S. forces and between U.S. forces and allied, multinational, and coalition forces. These lessons learned also highlight the continuing importance of interoperability to ensure the most efficient and effective future joint operations. In the vein of importance there are several other indicators. In addition to the obvious--that joint operations require joint command and control, which requires interoperability between the different services, systems--there is recognition of shortfalls and their impact on future operations, senior leadership's focus, and warfighter/CINCs' emphasis, to include naming an operational CINC as the advocate for interoperability.

Despite the recognition of its importance and the enormous efforts exerted toward achieving it, interoperability continues to elude the DOD. While it would be easier to fix if a single person, office, or institution were the culprit, in reality there is no single entity to blame. Instead the problem is attributed to the combinations of factors that contribute to the interoperability problems that continue to haunt U.S. joint operations. Among these factors are shrinking budgets, rapidly changing technology, changing nature of operations, lack of priority, lack of oversight, and unrealistic and infrequent joint training.

The good news is that the DOD continues to work aggressively to mitigate the impacts of the factors that make achieving interoperability difficult. During the past 18 months tremendous effort has resulted in the updates and promulgation of new visions mandating interoperability and policy that codify requirements for and methodology identifying interoperability KPPs and certification procedures for "all" automated information systems acquisition. Also, the organizational changes in the DOD hold promise of improving the prospects for achieving interoperability. By naming the newly designated JFCOM as the joint force "integrator" and "interoperability advocate" and assigning the operational command responsibilities for joint training and for reviewing and providing input to all systems acquisitions, the DOD now has a single operational warfighter charged with improving interoperability through training and to assuring interoperability of new systems.

6.2 What Does the Future Hold?

With the DOD's effort to mitigate the factors that plague attempts to achieve interoperability, will the department really be able to achieve interoperability? No one has a crystal ball and can say that with 100 percent certainty. However, it is probably safe to say that some of the factors discussed will continue to influence the pursuit of interoperability. In sticking with the guidelines of Harvard University Program on Information Policy no specific recommendations are made, but the following discussion is presented for consideration for the DOD's effort to achieve interoperability.

While the DOD has no control over some of the factors, it must continue to take steps to mitigate the associated circumstances, and for the ones that they can control they should take steps to eliminate them or reduce their effect. Future operations will continue to involve either joint U.S. forces or more likely allies, multinational, and coalition forces, which makes it essential that new systems be born joint, and that modifications to existing systems ensure joint interoperability. It is probably safe to say that the budgets will stay pretty much the same with the most optimistic being a slight increase in real time dollars. This necessitates that trade-offs be made smartly in coordination with the warfighters or operators and that interoperability be included in initial acquisitions to prevent more expensive, often unbudgeted, modifications after fielding. Technology is going to continue to change rapidly so the DOD must continue to seek innovative acquisition strategies such as the evolutionary approach to take advantage of the latest innovations. Also, the DOD must continue its attempt to define standards that ensure interoperability of the newest systems with the legacy systems of older generations of technology.

The DOD must continue aggressive efforts to mitigate the factors affecting interoperability that they do have control over. It must provide sufficient and effective oversight or the latest effort to update and promulgate visions and policy and guidance will have been for naught. The DOD and the services must ensure that the priority placed on interoperability is commensurate with its importance so that it prevails through trade-offs in capability and functionality. Joint exercises and training must be more frequent and realistic to ensure that the forces are ready for rapid "come as you are" deployments. Only through this realistic training will procedures be honed and shortfalls in doctrine, tactics, procedures, and equipment performance be identified so they can be corrected. Last, the DOD must find a way to tear down the barrier between the technicians and the operators so that the people responsible for the information systems understand the operational nature. Additionally, they must find a way to provide incentives to recruit and retain technically and operationally proficient people.

Perhaps we can learn from the final lesson learned in the Navy's lessons from the Persian Gulf War. "The naval forces and capabilities put to the test in Desert Shield/Desert Storm were not achieved by decisions made in the last few years…[they] were products of decisions made throughout the 1980s. So a final lesson might well be that the decisions we make today do have

important ramifications for the future."[1] That said, the decisions made today regarding interoperability will definitely impact its future and may well hold the key to answering the question, "Is it achievable?"

[1] U.S. Navy In Desert Shield/Desert Storm, VI Lessons Learned and Summary, Department of the Navy, Naval Historical Center, Washington D.C., http://www.history.navy.mil/wars/dstorm/ds6.htm, accessed January 02, 2001.